

REMARKS

In the Office Action, the Examiner rejected claims 1, 3-6, 9-11, 13-19, 22-27 and 29-40. By this Response, Applicants have amended claims 27 and 36, have canceled claims 39 and 40, and have added claim 41. No new matter has been added. As such, claims 1, 3-6, 9-11, 13-19, 22-27, and 29-38, and 41 are pending. In view of the following remarks, Applicants respectfully request reconsideration and allowance of all pending claims.

Claim Rejection Under 35 U.S.C. § 112, second paragraph

In the Office Action, the Examiner rejected claims 27 and 29-32 as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. More specifically, the Examiner stated:

Claim 27 recites the limitation “write the one or more bits to the seed pool” without explaining where said seed bits come from. The only mention of “seed bits” occurs a few lines previous wherein Applicant discloses “a non-volatile memory device to store a seed pool comprising a plurality of data bits.” It is unclear whether or not the seed bits being written to the seed pool are those disclosed with respect to the already existing seed pool filled with already existing bits, or whether the bits being written are additional bits, and wherein those bits come from.

Office Action, page 3. As suggested by the Examiner, Applicants have amended claim 27 to address any prior ambiguity. Specifically, the word “the” has been deleted from the limitation cited above, and the bits recited in the limitation have been designated as originating from a source external to the recited seed pool. Accordingly, Applicants respectfully request that the Examiner withdraw the rejection under Section 112, second paragraph.

Claim Rejections Under 35 U.S.C. § 102

In the Office Action, the Examiner rejected claims 13-18, 27, 29-32 and 35 under 35 U.S.C. § 102(b) as being anticipated by Utz et al., U.S. Patent No. 5,680,131 (hereafter referred to as “the Utz reference”). In addition, the Examiner rejected claims 36-40 under 35 U.S.C. § 102(b) as being anticipated by Bruce Schneier’s “Applied Cryptography” (hereafter “the Schneier reference”). Applicants respectfully traverse these rejections.

Legal Precedent

Anticipation under 35 U.S.C. § 102 can be found only if a single reference shows exactly what is claimed. *See Titanium Metals Corp. v. Banner*, 227 U.S.P.Q. 773 (Fed. Cir. 1985). For a prior art reference to anticipate under Section 102, every element of the claimed invention must be identically shown in a single reference. *See In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir.1990). That is, the prior art reference must show the *identical invention* “in as complete detail as contained in the . . . claim” to support a *prima facie* case of anticipation. *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989) (emphasis added). Thus, for anticipation, the cited reference must not only disclose all of the recited features but must also disclose the *part-to-part relationships* between these features. *See Lindermann Maschinenfabrik GMBH v. American Hoist & Derrick*, 221 U.S.P.Q. 481, 486 (Fed. Cir. 1984). Accordingly, Applicants need only point to a single element or claimed relationship not found in the cited reference to demonstrate that the cited reference fails to anticipate the claimed subject matter. A *strict correspondence* between the claimed language and the cited reference must be established for a valid anticipation rejection.

Moreover, the Applicants submit that, during patent examination, the pending claims must be given an interpretation that is *reasonable* and *consistent* with the specification. *See In re Prater*, 162 U.S.P.Q. 541, 550-51 (C.C.P.A. 1969); *In re Morris*, 44 U.S.P.Q.2d 1023, 1027-28 (Fed. Cir. 1997); *see also* M.P.E.P. § 2111 (describing the standards for claim interpretation during prosecution). Indeed, the *specification* is “the primary basis for construing the claims.” *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005). It is usually dispositive. *See id.* Interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach. *See In re Cortright*, 49 U.S.P.Q.2d 1464, 1468 (Fed. Cir. 1999); *see also* M.P.E.P. § 2111. That is, recitations of a claim must be read as they would be interpreted by those of ordinary skill in the art. *See Rexnord Corp. v. Laliram Corp.*, 60 U.S.P.Q.2d 1851, 1854 (Fed. Cir. 2001); *see also* M.P.E.P. § 2111.01. In summary, during prosecution an examiner must interpret a claim recitation as one of ordinary skill in the art would reasonably interpret the claim in view of the specification. *See In re American Academy of Science Tech Center*, 70 U.S.P.Q.2d 1827 (Fed. Cir. 2004).

The Utz Reference Lacks Features Recited in Independent Claims 13 and 27

Claim 13 recites, *inter alia*, “A method of initializing a seed pool . . . comprising the acts of: (a) prior to enabling the cryptographic security subsystem, writing a plurality of bits of data to a seed pool, the plurality of bits having a signature value . . . (c) writing one or more bits to the seed pool upon termination of the first type of triggering event, the one or more bits of data *altering the signature value of the seed pool*; [and] (d) enabling the cryptographic security subsystem when more than a predetermined portion of the signature value of the seed pool has been altered.” (Emphasis added). Currently amended claim 27 recites, *inter alia*, “A processor-based device comprising . . . a non-volatile memory device to store a seed pool comprising a plurality of data bits; and security logic in communication with . . . the non-volatile memory device . . . wherein the security logic is configured to: write one or more bits to the seed pool, wherein the bits originate from a source external to the seed pool and *alter a signature value*; determine whether a plurality of data bits in the seed pool has at least a portion of the signature value; and disable establishment of the secure communication session if the plurality of data bits has at least a portion of the signature value.” (Emphasis added).

In contrast, the Utz reference does not teach or suggest altering a signature value to determine when to enable a cryptographic security subsystem, as recited in claims 13 and 27. In rejecting claims 13 and 27, the Examiner correlated the “start value” of the Utz reference with the “signature value” of the present claims. *See* Office Action, p. 4. The correlation of the start value of Utz and the signature value of the present claims is only accurate insofar as they each comprise bits. Indeed, the start value bits are used for entirely different purposes than the signature value bits, and thus there is no significant correlation between the start value and the signature value.

Specifically, while the signature value of the present claims is altered when one or more bits are written to the seed pool, the start value of the Utz reference is never altered. Rather, the start value is used as an identifying value for a receiver to recognize a remote transmitting device. *See* Utz, col. 6, line 65 to col. 7, line 18. The Utz reference discloses a transmitting unit that relays start values to a receiving unit, and these relayed start values are compared with corresponding start values from the receiving unit to determine whether they

match. *See id.* For such a comparison to be accomplished, it is necessary that the start values are fixed. *See id. at col. 8, lines 58-63.* In fact, to preclude alteration of the start value, the nonvolatile memory in which the start value is stored is made one-time programmable by a disable fuse. *See id. at col. 8, line 58 to col. 9, line 4.*

Thus, the Utz reference does not disclose altering a signature value, as set forth in independent claims 13 and 27. Accordingly, Applicants respectfully request that the rejection of claims 13 and 27 and their respective dependent claims be withdrawn.

The Schneier Reference Lacks Features Recited in Independent Claim 36

Currently amended claim 36 recites, *inter alia*, “A method for restoring security data to non-volatile memory in a computer system comprising: . . . tracking the state of the seed pool to determine if the seed pool is fully populated, wherein tracking the state of the seed pool comprises *examining a state bit that changes states when the seed pool is fully populated or examining the position of a pointer to determine whether the portion of the non-volatile memory storing the seed pool is full*” (emphasis added).

In contrast, the Schneier reference fails to disclose examining a state bit or the position of a pointer to determine whether a seed pool is full. The Schneier reference addresses the problem of populating a seed pool in the absence of triggering events between system reboots. *See Schneier*, page 428, lines 16-18. However, rather than suggesting a method for solving this problem, the author states that “there is *no solution to this problem other than to wait* until enough external random events have taken place.” *See id.* (emphasis added). Applicants believe the cited passage is absent of any language teaching or suggesting determining when a seed pool is full by use of a state bit, a pointer position, or by any other method. Indeed, the Examiner concedes this deficiency in a prior Office Action, providing that “Schneier fails to *specifically* mention determining if a seed pool is full.” *See Office Action Mailed on November 29, 2006, page 9* (emphasis in original).

Moreover, although the Schneier reference refers to a “buflen” variable (a defined variable in a high level programming language) that is used in a subroutine to determine

whether a buffer is full, using such a variable is not the equivalent of examining a state bit or the position of a pointer to determine whether the portion of a non-volatile memory storing a seed pool is full. The “buflen” variable disclosed in Schneier is provided as part of a `genrand()` function written in a high-level programming language. *See* Schneier, page 427. In the `genrand()` function, the “buflen” variable is a numerical value that is decremented as a buffer is filled. *See* Schneier, page 427. As such, the “buflen” variable cannot reasonably be considered to be the same as a state bit or a pointer position, as set forth in the instant claims.

Thus, the Schneier reference fails to teach or suggest examination of a state bit or examination of a pointer position, as set forth in independent claim 36. Accordingly, Applicants respectfully request that the rejection of claim 36 and its dependent claims be withdrawn.

Rejections Under 35 U.S.C. § 103(a)

In the Office Action, the Examiner rejected claims 1, 3-6, 9-11, 19, 22-26, and 33-34 under 35 U.S.C. § 103(a) as being unpatentable over the Schneier reference and further in view of the Utz reference. Applicants respectfully traverse this rejection.

Legal Precedent

The burden of establishing a *prima facie* case of obviousness falls on the Examiner. *Ex parte Wolters and Kuypers*, 214 U.S.P.Q. 735 (B.P.A.I. 1979). In supporting this burden, it is often necessary “to look to interrelated teachings of multiple patents, the effects of demands known to the design community or present in the market place; and the background knowledge possessed by a person having ordinary skill in the art.” *KSR Int’l Co. v. Teleflex, Inc.*, 550 U.S. ____ (2007). Indeed,

Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented.

Id. (quoting *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1 (1996)). This analysis should be made explicit. *Id.* (citing *In re Khan*, 441 F.3d 977, 988 (Fed. Cir. 2006) (“[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness”)).

Moreover, a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was known in the prior art. *See id.* As such, the obviousness inquiry does not hinge on demonstrating that elements were known in the art. Rather, the obviousness inquiry should focus on whether, in view of the demands and knowledge of the design community at the time of filing the application, without hindsight bias, what is claimed would have been obvious to persons having ordinary skill in the art. *See id.*

The Utz and Schneier References, Taken Alone or in Hypothetical Combination, Fail to Disclose All Elements of Independent Claims 1 and 19

Claim 1 recites, *inter alia*, “writing one or more bits of data to a seed pool upon termination of the first type of triggering event, the seed pool comprising a *state bit indicative of a state of the seed pool . . . [and] examining the state bit to determine whether the seed pool is full.*” (Emphasis added). Claim 19 recites, *inter alia*, “a non-volatile memory device to store a seed pool, wherein the seed pool comprises a *state bit indicative of the state of the seed pool . . . and security logic . . . configured to . . . examine the state bit to determine whether the seed pool is fully populated.*” (Emphasis added).

As previously discussed, the Schneier reference fails to teach or suggest examining a state bit to determine if a seed pool is fully populated. In fact, as mentioned above, the Examiner conceded that Schneier fails to specifically teach or suggest the act of determining whether a seed pool is full.

Moreover, the Utz reference fails to obviate the deficiencies of the Schneier reference. The Utz reference is directed to a transmitting unit of a wireless security system. *See Utz*, col. 3, line 19. A pseudo-random number generator is used to generate a randomized

synchronization code that is transmitted to a receiving unit. *See id.* at col. 3, lines 20-22. Verification codes are then generated by incrementing the pseudo-random number generator. *See id.* at col. 3, lines 22-40. The Utz reference also discusses some variable features of the transmitting unit, including the possibility of generating different synchronization codes after successive applications of power. *See id.* at col. 11, lines 50-55. However, the Utz reference *never* mentions examining a state bit to determine whether a seed pool is full. Indeed, the Utz reference does not even disclose a state bit.

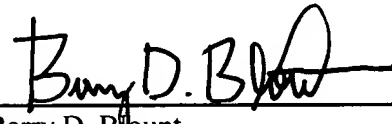
Thus, the Utz and Schneier references, taken alone or in hypothetical combination, fail to teach or suggest examining a state bit to determine if a seed pool is fully populated, as set forth in independent claims 1 and 19. As such, a *prima facie* case for obviousness under 35 U.S.C. § 103 has not been presented. Accordingly, Applicants respectfully request that the rejection of claims 1 and 19 and their respective dependent claims be withdrawn.

Conclusion

Applicants respectfully submit that all pending claims are in condition for allowance. However, if the Examiner wishes to resolve any other issues by way of a telephone conference, the Examiner is kindly invited to contact the undersigned attorney at the telephone number indicated below.

Respectfully submitted,

Date: August 16, 2007


Barry D. Blount
Reg. No. 35,069
FLETCHER YODER
(281) 970-4545

Correspondence Address:

IP Administration
Legal Department, M/S 35
HEWLETT-PACKARD COMPANY
P.O. Box 272400
Fort Collins, CO 80527-2400